CLAIMS

1. A computing device comprising:

a processing system;

an externally-accessible memory coupled to the processing system;

a secret identification number generated for the computing device and stored in a secure memory that is not externally-accessible;

a key generator for generating a random key associated with a selected electronic file to be stored in the externally-accessible memory;

a symmetrical encryption system to generate an encrypted key by symmetrically encrypting the random key using the secret identification number;

wherein the processing system associates a digital certificate with the electronic file, where the digital certificate contains the encrypted key, such that the electronic file can be accessed only after the processing system restores the random key through decryption of the encrypted key with the secret identification number.

2. The computing device of claim 1 wherein digital certificate comprises contains a software signature that is symmetrically encrypted using the random key.

3. The computing device of claim 2 wherein the software signature comprises a hash of the electronic file, where the hash is symmetrically encrypted using the random key.

4. The computing device of claim 2 wherein the digital signature further contains a signature for selected fields of the digital certificate, wherein the selected fields of the digital certificate are coded and encrypted using the random key.

5. The computing device of claim 1 wherein the electronic file is symmetrically encrypted using the random key.

6. The computing device of claim 1, wherein the encoded key is stored in the externally-accessible memory.

7. A method of providing security to files stored in an externally-accessible memory of a computing device comprising the steps of:

storing a secret identification number for the computing device in a secure memory that is not externally-accessible;

generating a random key;

generating an encoded key by symmetrically encrypting the random key using the secret identification number;

associating a digital certificate with the electronic file, where the digital certificate contains the encrypted key, such that the electronic file can be accessed only after restoring the random key through decryption of the encrypted key with the secret identification number.

8. The method of claim 7 wherein the associating step includes the step of generating a software signature encrypted using the random key and storing the software signature in the digital certificate.

9. The method of claim 8 wherein the generating step comprises the step of generating a hash of the electronic file, where the hash is symmetrically encrypted using the random key.

10. The method of claim 8 wherein the associating step includes the step of generating a signature for selected fields of the digital certificate, wherein the selected fields of the digital certificate are coded and encrypted using the random key.

11. The method of claim 7 and further comprising the step of encrypting the electronic file using the random key.

12. The method of claim 7 and further comprising the step of storing the encoded key in the externally-accessible memory.

13. The method of claim 7 and further comprising the step of symmetrically decrypting the encoded key using the secret identification number upon a request to access the electronic file.

14. The method of claim 13 and further comprising the step of decrypting one or more fields of the digital certificate using the encoded key.

15. The method of claim 14 and further comprising the step of decrypting an encrypted electronic file using the encoded key.

16. A method of storing a protected file in an externally-accessible memory of a computing device comprising the steps of:

storing a secret identification number for computing device in a secure memory that is not externally-accessible;

generating a random key associated with a selected electronic file to be stored in the externally-accessible memory;

generating an encoded key by symmetrically encrypting the random key using the secret identification number;

encrypting the selected electronic file using the random key and storing the encrypted electronic file in the externally-accessible memory; and

storing the encrypted key in the externally-accessible memory and associating the encrypted key with the encrypted electronic file, such that the encrypted electronic file can be decrypted only after restoring the random key through decryption of the encrypted key with the secret identification number.

17. The method of claim 16 and further comprising the step of storing an encrypted software signature for the electronic file in the externally-accessible memory, where the software signature is a hash of the electronic file, encrypted using the random key.